SoK: P2PWNED — Modeling and Evaluating the Resilience of Peer-to-Peer Botnets

IEEE Symposium on Security and Privacy,2013

本文中，引入一个图解模型捕捉P2P僵尸网络的内在性质和基本的安全漏洞，使用这个模型来评定现在P2P僵尸网络对攻击的恢复力，评估了十一个活跃的P2P僵尸网络，通过分析结果来帮助安全研究人员评估减灾策略应对当前以及之后的P2P僵尸网络。

Finding the Linchpins of the Dark Web: a Study on Topologically Dedicated Hosts on Malicious Web Infrastructures

IEEE Symposium on Security and Privacy,2013

文章中使用了来自各种攻击方式的四百万个恶意的URL，展示了数量极大的主机在恶意的行为中的拓扑关系，发现了一些只用于恶意的而不访问正常站点的主机。发明了一种基于图的方法，将已知的少量只用于恶意的主机作为种子在打的范围内检测恶意的主机。

Domain-Z: 28 Registrations Later

IEEE Symposium on Security and Privacy，2016

文章说了一个域名剩余信用滥用（residual trust abuse）的问题，恶意的注册一个过期的域名，利用域名之前使用存留的正当记录。

EXPOSURE: Finding Malicious Domains Using Passive DNS Analysis

NDSS Symposium，2011

提取15种特征值，利用机器学习的方法进行恶意域名检测

Ghost Domain Names: Revoked Yet Still ResolvableNDSS Symposium，2012

展示了在上级DNS服务器上检测恶意域名是不可行的，并提出几种应对这些ghost domain names的办法。

Parking Sensors: Analyzing and Detecting Parked Domains

NDSS Symposium，2015

这篇文章从安全的角度展示并探究了域名停靠的生态系统，分析了域名所有者、停放服务和涉及到的广告提供商。期间发现了许多域名利用误植域名，侵犯了其他的网站或是商标。文章提出了一系列的特征来代表停放的域名，分类器很精确。

Detecting Malware Domains at the Upper DNS Hierarchy

USENIX Security Symposium，2011

提出了一个叫做Kopis的恶意软件相关域名的检测系统。Kopis被动监控DNS流量，通过分析全局DNS查询模式精确检测恶意域名。EXPOURE监控的是本地递归DNS服务器的，Kopis监控上级DNS服务器，更有全局性。Kopis检测优点还有不需要其他网站数据，可以独立对DNS操作，不需要IP reputation information。

BOTMAGNIFIER: Locating Spambots on the InternetUSENIX Security Symposium，2011

提出一种新的技术来识别和追踪发送垃圾邮件的僵尸主机。首先将垃圾邮件主机的IP地址作为输入，并对这些主机的行为进行学习，然后通过大量的邮件传输日志放大行为特征来识别互联网上其他主机的行为。

From Throw-Away Traffic to Bots: Detecting the Rise of DGA-Based Malware

USENIX Security Symposium，2012

针对使用DGA算法的僵尸网络进行检测，可以精确检测被感染主机，发现新的DGA（Domain Generation Algorithm）算法，还会建立起新的模型，并识别CNC服务器. 使用DGA一个种子会产生大量的域名，其中一个是CNC域名，而其他域名都是无效的，受感染主机在寻找CNC服务器的同时会产生大量无效的域名，即NXDomain。同一个DGA产生的域名是相似的，通过机器学习的方法，可以建立起有关DGA的模型，进一步检测到CNC服务器。

ExecScent: Mining for New C&C Domains in Live Networks with Adaptive Control Protocol Templates

USENIX Security Symposium，2013

文章提出一种新的系统，使用活跃的网络流量来检测新型的未知的C&C域名，叫做ExecScent。ExecScent利用已知的C&C服务器通信，学习控制协议模版，产生混合模版自动调整针对不同的环境，是第一个适应C&C流量的系统。

A Comprehensive Measurement Study of Domain Generating Malware

USENIX Security Symposium，2016

文章对使用DGA的恶意软件做了综合性的分析，展示了DGA的分类并提出特征相互比较。通过重现算法，预先计算了所有可能产生的域名，覆盖了大多数已知的DGA算法。然后研究了一千八百万个DGA域名的注册状态，结果显示相关的恶意软件族及其活动都在这些计算好的域名中。

The Ever-Changing Labyrinth: A Large-Scale Analysis of Wildcard DNS Powered Blackhat SEO

USENIX Security Symposium，2016

首先渗透进入到一个蜘蛛池，建立一个检测系统探索所有的SEO域名是如何组织的。然后利用蜘蛛池的独有特征，开发了一个扫描器找到SEO域名。最后测量蜘蛛池生态系统并分析从21个蜘蛛池爬到的结果。